
Erik Neitzel
Faculty of Informatics, Otto-von-Guericke-University of Magdeburg, Magdeburg, Germany, erik.neitzel@ovgu.de
Department of Business and Management, Brandenburg University of Applied Sciences, Brandenburg an der Havel, Germany, neitzel@fh-brandenburg.de

André Nitze
Department of Cooperative Studies, Berlin School of Economics and Law, Germany, andre.nitze@hwr-berlin.de

Sachar Paulus
Department of Business and Management, Brandenburg University of Applied Sciences, Brandenburg an der Havel, Germany, paulus@fh-brandenburg.de

Abstract

Within this article, an integrated framework for the development of GRC-optimized business processes is developed based on other business process and GRC management frameworks. Its goal is to analyse, design, implement, monitor and optimize business processes from a GRC perspective. Information security criteria shall be used to demonstrate its effectiveness regarding a mobile supported, federated End-to-End business process, the Order-to-Cash (OTC). While traditional approaches address symptoms of GRC incidents, the framework at hand shall address their origin, which lies in the specific nature of work performed within each business process. Most importantly, common information security specific frameworks focus on the implementing organization only, which results in a lack of effectiveness for federated business scenarios. A new framework addresses this problem in particular by aggregating risk analysis results across organizations.

(1) Situation, setting and aim of this paper

In today’s business environments, the need for product innovation is growing more and more to stay competitive. Product innovation within highly unstable markets demand increasing virtualization within organizations to execute defined business processes across those organizations. This is achieved by federations, meaning horizontal (organizations within the same market) and vertical (organizations in different markets but mutual benefits, e.g. hotels providing free WLAN) cooperations. Technical requirements for flexible business processes evolve with the evolution of IT architectures from client/server to workflows to middleware to cloud services. This helps reducing the complexity of information technology. But, at the same time, the necessity of handling Governance, Risk and Compliance (GRC) requirements such as information security and conformity with regulatory requirements remains unchanged. The
complexity to handle those requirements, however, increases when dealing with federations and cross-company end-to-end business processes.

Classical approaches towards GRC management such as frameworks like COBIT 5.0 [Ins12], ITIL v3 [Klo08] and ISO 27001 [ISO13] operate within clearly defined organizational borders. Results of those frameworks are controls to be implemented within a pre-defined organizational setting consisting of various human and IT-related resources. One can argue that they address the symptoms of flawed business process design instead of coping with GRC related issues that arise within a business process context. This paper aims to take this view into account and proposes an approach to tackle GRC related requirements within a cross-company business process context.

The first thesis of this paper is that traditional GRC frameworks cannot be used to effectively address federated business scenarios. This thesis shall be analyzed and demonstrated within the scope of the Order-to-Cash end-to-end business process (OTC), because this example scenario is (a) complex enough [EN13] and (b) used within almost any organizational setting, since it belongs to most organizations’ value chains. Afterwards, a new framework for design, implementation and controlling of GRC optimized business processes is developed. To evaluate the framework developed, the OTC shall be defined within a specific technical environment to be able to work with dedicated, specific controls. For the purpose of this paper, this environment shall consist of mobile supported OTC modules, whereas each module represents a standalone-capable part of the overall end-to-end business process. This setting was chosen because there is no consistent controls set defined to assure security within mobile business processes supporting various risk levels. Therefore, the design of such a control set is also part of the report at hand.

(2) Traditional approaches

[Here, a comparison of traditional GRC relevant approaches took place. Regarding the purpose of this survey, this is not relevant and was cut out to simplify reading the article.]

All of the GRC frameworks mentioned address the symptoms of insufficient business process design. That design results either in potentially insecure and incompliant business processes, especially regarding federated end-to-end scenarios, or in massive investments to build and manage the controls necessary according to these frameworks. ISO 27001 shall be used for further analysis of those federated business processes as it represents a common approach for dedicated information security management. Furthermore, it allows for enough flexibility (since it does not prescribe a concrete set of controls) but still is precise enough with respect to the protection goals.

(3) Executing ISO 27001 on a mobile supported Order-to-Cash Business Process

To understand the lack of effectivity of GRC management using traditional methodologies, and to evaluate a newly designed framework later on, a concrete, federated end-to-end business process example shall be provided.
(3.1) The business scenario

To demonstrate the value of a framework, its reference point should be both prevalent and complex. Therefore, the Order-to-Cash (OTC) business process shall be separated into business process modules. Afterwards, the classical approach of ISO 27001 shall be executed for one of those business process modules. A business process module is hereby a receipt producing and/or receiving element of the business process. Federation could take place between two of such business process modules, see figure 1.

![Diagram of Procure-to-Pay - Order-to-Cash interactions](image)

To get closer to outlining the problem, the deliverables of ISO 27001 shall now be collected for the described OTC scenario. As a means of simplification, the OTC shall once be seen from the perspective of an OTC provider (the creditor carrying out the OTC) and an OTC user (the debtor carrying out its procure-to-pay or PTP business process, thereby using the OTC of the creditor). This helps understanding the different points of view regarding information risk management. Of course a federated OTC itself also carries similar controversy business information from one business process module to another.

We will now focus on the order information, addressing an early step of the PTP/OTC interaction. A business-driven way of using ISO 27001 would result in delivering a table showing business process modules, critical information, supported IT systems, protection requirements, threats and risk assessments for information being carried across the federation as a core deliverable within phase 1 “Definition of an Information Security Management System”.

(3.2) Definition of an Information Security Management System based on ISO 27001
The following steps shall be executed:

A. **Scope definition:** Order-to-Cash business process and all its information based assets and mobile support resources (disregarding their actual physical location)

B. **Definition of an ISMS policy** (expected as given, for the entire organization)
   - main goal: being able to assess risks towards OTC related information being transmitted through mobile resources
   - general business related and legal requirements which will be shown in tables 2 and 3;
   - integration with strategic risk management processes is given
   - criteria for assessing risks: assets, threats, weak points, consequences
   - approval of management is given

C. **Definition of risk assessment approach**
   - Criteria for risk handling: here: qualitative delimitation: normal (no special protection need), high, very high (huge protection need)

D. **Identification of risks** (see tables 2 and 3) by identifying:
   - assets
   - threats
   - weak points
   - consequences

E. **Analysis and assessment of risks** (see tables 2 and 3)
   - Assessment of business damage
   - Assessment of probability of occurrence
   - Assessment of resulting current risk level
   - Decision of either accepting risk or treating risks

The steps (1) (D) and (1) (E) will result in different content for each of the organizations in question: the organization providing the OTC and the organization using that OTC through their procurement cycle, see tables 2 and 3. The critical controversy regarding information risk management is marked bold.

F. **Identification and assessment of options for risk assessment**;
   Possible actions:
   - Implementation of controls (no specific controls present for mobile scenario)
   - Acceptance of risk
   - Avoidance of risk
   - Transfer of risk

G. **Choice of controls and their goals**: due to a lack of mobile controls, there is no way of choosing present controls, it becomes a matter of designing them.

H. Agreement of management is not given until controls are defined.
I. Approval of management pending until controls and their costs are determined.
J. **Statement of applicability** is given, stating
   - the reason for certain controls and their goals
   - currently existing controls
   - exclusion of controls of appendix
(3.3) Perspective: Order-to-Cash Provider

For an OTC provider, incoming order data will often be subject of no further risk assessment, or of assessing the risk as low, compared to other information of the OTC provider’s overall business, since transmitted information are not considered critical, see table 2.

<table>
<thead>
<tr>
<th>#</th>
<th>Business Process Module</th>
<th>Information asset (Receipt)</th>
<th>Supported IT system</th>
<th>Protection requirement</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Receive RFQ</td>
<td>RFQ</td>
<td>SAP ERP, mobile Interface</td>
<td>Normal</td>
<td>None perceived</td>
</tr>
<tr>
<td>2</td>
<td>Send quotation</td>
<td>Quotation</td>
<td>SAP ERP</td>
<td>High</td>
<td>Compromised confidentiality towards competitors</td>
</tr>
<tr>
<td>3</td>
<td>Receive order</td>
<td>Order</td>
<td>SAP ERP, mobile Interface</td>
<td>Normal</td>
<td>None perceived</td>
</tr>
<tr>
<td>4</td>
<td>Send confirmation</td>
<td>Order confirmation</td>
<td>SAP ERP</td>
<td>Normal</td>
<td>Legal issue</td>
</tr>
<tr>
<td>5</td>
<td>Send availability state</td>
<td>Availability state</td>
<td>SAP ERP</td>
<td>Normal</td>
<td>None perceived</td>
</tr>
<tr>
<td>6</td>
<td>Send delivery note</td>
<td>Delivery note</td>
<td>SAP ERP</td>
<td>Normal</td>
<td>None perceived</td>
</tr>
<tr>
<td>7</td>
<td>Send invoice</td>
<td>Invoice</td>
<td>SAP ERP</td>
<td>High</td>
<td>Main business concern, data integrity violations</td>
</tr>
<tr>
<td>8</td>
<td>Receive payment</td>
<td>Payment data</td>
<td>SAP ERP, mobile Interface</td>
<td>Very high</td>
<td>Main business concern</td>
</tr>
</tbody>
</table>

Table 2: Order-to-Cash Provider’s Risk Assessment

(3.4) Perspective: Order-to-Cash User

However, for an OTC user, e.g. Apple or BMW, order information, meaning the order receipt, can be considered high risk information, since it could allow drawing conclusions regarding future product development, see table 3.

<table>
<thead>
<tr>
<th>#</th>
<th>Business Process</th>
<th>Information asset</th>
<th>Supported IT system</th>
<th>Protection requirement</th>
<th>Threats</th>
</tr>
</thead>
</table>

Table 3: Order-to-Cash User’s Risk Assessment
<table>
<thead>
<tr>
<th>Module</th>
<th>(Receipt)</th>
<th>ment</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Send RFQ</td>
<td>RFQ</td>
<td>openERP</td>
</tr>
<tr>
<td>2</td>
<td>Receive quotation</td>
<td>Quotation</td>
<td>openERP, mobile Interface</td>
</tr>
<tr>
<td>3</td>
<td>Send order</td>
<td>Order</td>
<td>openERP</td>
</tr>
<tr>
<td>4</td>
<td>Receive confirmation</td>
<td>Order confirmation</td>
<td>openERP, mobile Interface</td>
</tr>
<tr>
<td>5</td>
<td>Receive availability state</td>
<td>Availability state</td>
<td>openERP, mobile Interface</td>
</tr>
<tr>
<td>6</td>
<td>Receive delivery note</td>
<td>Delivery note</td>
<td>openERP, mobile Interface</td>
</tr>
<tr>
<td>7</td>
<td>Receive invoice</td>
<td>Invoice</td>
<td>openERP, mobile Interface</td>
</tr>
<tr>
<td>8</td>
<td>Send payment</td>
<td>Payment data</td>
<td>openERP</td>
</tr>
</tbody>
</table>

Table 3: Order-to-Cash User’s Risk Assessment

After having planned the ISMS, the next phase “Execution of the ISMS” would include executing it, including the formulation of a risk handling plan, realization of controls, definition of measurement and administration of the ISMS’ operation. Afterwards the phase “Monitoring of the ISMS” includes execution of validation processes and regular checks of the effectivity of ISMS. The last phase “Improvement of the ISMS” includes the realization of ISMS optimizations and reporting of controls and optimizations to stakeholders to ensure that all requirements meet the goals defined earlier.

The focus for the paper at hand, however, shall lie on phase 1 “Definition of an Information Security Management System”, as this phase carries the origin of risk controversy regarding federated business process information. At first, however, the following paragraph shall discuss the problem related to ISO 27001 within federated scenarios.

(4) Problem discussion

As seen in paragraph 2, there are different frameworks present for addressing GRC
requirements without being able to influence the business process where GRC issues come from. Interestingly, the opposite is also true: frameworks for building business processes do not address GRC requirements.

(4.1) General problems

All solutions for methodically addressing GRC management needs are laid out for usage within well-defined organizational borders. Some standards are mandating specific measures for extending the governance to suppliers (ISO 28000, for example), but in general it is impossible to efficiently use those methodologies for federated business process scenarios, as seen in paragraph 3.

Even within non-federated scenarios the fact that sustaining risk management needs to be based on managing business processes, is present. Within federated scenarios, however, the business process is the only thing connecting each organization taking part in the federation. Therefore GRC methodologies should begin at this point.

Even though some business process management methodologies for handling governance and compliance within business processes have been presented by Markus and Jacobsen [MM10], present business process frameworks do not fully address GRC requirements – especially in terms of information security risks.

(4.2) Current business process management frameworks

Business process management is no longer a tool for just designing work packages, sequentially aligned to serve effectivity and efficiency regarding business purposes. Today’s business process management has to serve the purpose of deriving processes from business goals and external success and risk factors. Additionally, process management has to consider potentials and threats towards people, services and technology supporting each business process. Business processes are planned and implemented and subsequently each business process can be measured and optimized.

There are already different business process frameworks present. One of those frameworks is the ARIS process management lifecycle [Sch00]. ARIS is a tool to map the business strategy into business processes with regards to effectivity and efficiency. Among a number of tools and description languages, ARIS has reached a prominent acceptance in the industry across all vertical sectors. In ARIS’ methodological approach, business processes are derived from business goals and external success factors, their potential and threats are analyzed, processes are planned and implemented and subsequently each process can be measured and optimized. On the other hand, ARIS does not address GRC requirements.

There are other business related frameworks as the McKinsey 7s framework addressing structure, strategy, systems, skills, style, staff and shared values [T84]. McKinsey’s 7s framework is a management model meant to assess business related changes while internal changes take place within an organization. This can be seen as a special diagnosis tool for change management processes.

Other business process frameworks are present, to name a few:

- MIT Process Handbook [OT03]
- OPEN Process Framework [OP09]
Yet none of the existing business frameworks sufficiently cover GRC requirements, especially regarding federated end-to-end business processes. Therefore we propose to develop a business process management framework for federations, which takes GRC requirements into consideration prior to building the business process.

Such a framework has relevance since the trend for federations will probably continue due to the rising necessity of dynamically changing business processes whilst staying secure and compliant in continuously changing market situations. This complexity calls for a GRC-enhanced business process framework, which shall be constructed within the following paragraph.

(5) Design of a GRC optimized business process framework

How shall the work of GRC processes be designed in order to produce secure business process designs? A prudent way to obtain the perspective of a business process towards its surroundings can be extrapolated of the views of ARIS [EI08].

(5.1) Basic framework structure

ARIS, however, focuses on effectivity and efficiency of business processes only. Yet at the absence of GRC relevant requirements, those views shall be extended to the following:

- Resources view: business process related employees, applications, infrastructure and their relationships
- GRC function view: activities capable of designing input for building and influencing business processes
- GRC data view: requirements (restrictions and obligations towards both functions and data usage), key performance indicators (KPI), monitoring and other data needed to process GRC functions
- GRC process view: using GRC functions and GRC data to deliver business process design
- Business function view: transactions/activities that use business data by a well-defined way (work packages)
- Business data view: business information objects and their attributes, as well as the relationships between those objects
- Business process module view: view combining GRC input for process specification using business functions and business data as well as resources produce products and services
- Services and products view: output of business processes

Figure 2 illustrates that GRC-enhanced business process framework blueprint.
(5.2) Framework phases

The following overview shall describe the GRC-enhanced way in which the views above shall be integrated into one another using the five phases of analysis, design, implementation, monitoring and adjustment of business processes, see table 4. Phases added to ARIS process lifecycle are emphasized bold.

<table>
<thead>
<tr>
<th>#</th>
<th>GRC enhanced Business Process Management Framework Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Phase deliveries</td>
</tr>
<tr>
<td>1</td>
<td>BUSINESS PROCESS ANALYSIS</td>
</tr>
<tr>
<td></td>
<td>Scope definition</td>
</tr>
</tbody>
</table>
Analysis of business process and its identification within business process landscape and portfolio including determination of process costs

Analysis of potential, success and disturbance factors

Analysis of GRC requirements
  - Analysis of GRC-relevant (critical) business information
  - Analysis of regulatory obligations
  - Analysis of protection requirements
  - Analysis of threats
  - Analysis of current resource configuration (organizational and technical resources)

Analysis of business goals

Analysis of IT goals

2 BUSINESS PROCESS DESIGN

Address federative design aspects
  - Segmentation of business process into desired business process modules
  - Reference modules to organizations

Determine federation protection requirements
  - Walk through each critical business information (within a business process module)
  - Switch perspectives for each organization, business process module and critical business information
  - Select the highest protection requirement value of each perspective regarding the same critical information

Perform risk analysis for identified threats and critical information, thereby assessing already implemented controls

Design business process module draft
  - Address disturbance factors as business risks
  - Address potential and success factors
  - Design organizational structure based on work packages, necessary roles/profiles and employee competences
  - Design technical resource configuration (e.g. selection of cloud type and services) for current business process module

Design GRC controls
  - Control generation
    - Consider each business processes critical information and GRC requirement (e.g. very high protection requirement regarding confidentiality of information XYZ)
    - Select control and intensity to be addressed for each process modules technical resources
    - described within the following paragraphs
  - Control validation (mapping of controls against threats that have been identified earlier)
  - Derive specific technical controls based on the actual technical resource configuration
Table 4: New GRC-optimized business process framework

Phase 1 (analysis) is a combination of classical approaches from each business, IT and GRC management methodologies. Business needs, resource configuration and risk assessment are to be performed for every federated end-to-end business process.

The deliverables of phase 2 (design) emphasize the importance of switching perspectives for each business process module regarding risk assessment. Protection requirements shall
hereby be cumulated so that the higher value of each party taking part in the federation shall be used to select specific controls. First, general controls are derived by mapping GRC requirements of each process module against a pre-defined control set, e.g. from ISO 27001 (appendix) or the Unified Compliance Framework (UCF) [Fro13]. From there, specific controls can be derived based on the determined protection requirement level, which defines the intensity of a control.

Within phase 3 (implementation), those specific controls are to be implemented at each of the resources that have also been selected and/or identified earlier. Hence, GRC-related business process optimization is achieved by implementing technical controls being derived from general controls needed to handle the risks towards business information assessed earlier. The Phases 4 (monitoring) and 5 (adjustment) are common framework phases, but do not address business or IT or GRC issues only, but all of them in a combined way.

(5.3) Matching Business Process Modules to Controls based on GRC requirements

Within the design phase, controls are derived from GRC requirements of each critical information of each business process module. Table 5 shows exemplary general controls and their addressed GRC requirements. Note that the compliance aspect (e.g. auditability) is dependent on the business policies and external regulations and therefore cannot be prescribed by the control set.

<table>
<thead>
<tr>
<th>#</th>
<th>Control based on ISO 27001 appendix and/or Unified Compliance Framework</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Restrict user access</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>(x)</td>
</tr>
<tr>
<td>2</td>
<td>Encrypt data transmissions</td>
<td>x</td>
<td>x</td>
<td></td>
<td>(x)</td>
</tr>
<tr>
<td>3</td>
<td>Encrypt data storage</td>
<td>x</td>
<td>x</td>
<td></td>
<td>(x)</td>
</tr>
<tr>
<td>4</td>
<td>Set up redundancies</td>
<td></td>
<td>x</td>
<td></td>
<td>(x)</td>
</tr>
<tr>
<td>5</td>
<td>Establish information security guideline</td>
<td></td>
<td></td>
<td></td>
<td>(x)</td>
</tr>
<tr>
<td>6</td>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td>(x)</td>
</tr>
</tbody>
</table>

Table 5: Control and information security requirement matrix

This control set helps a framework to generate control suggestions based on risk analysis of the business process at hand. Those controls must then be scaled towards the specific protection requirement of each process module. However, mobile scenarios are not sufficiently covered with specific corresponding controls, which is why the next chapter shall define a set of specific controls for mobile application usage within federated business scenarios. Those specific controls correspond to the more general controls described here.

[Here, an evaluation based on a mobile supported Order-to-Cash business process took place using a self-developed specific control set that corresponds to the general]
controls mentioned above. Regarding the purpose of this survey, this is not relevant and was cut out to simplify reading the article.]

(8) Conclusion

Within this article, an integrated framework for the development of GRC-optimized business processes was built based on other business process and GRC management frameworks. Its scope ranges from the analysis of a business processes environment, its separation into federative business process modules, resource reconfiguration and control selection as well as implementation, monitoring and optimization of business processes. In addition, a specific set of controls for the purpose of handling mobile business process support was developed.

The overall construct could be positively evaluated at both a plain and a federated Order-to-Cash End-to-End business process scenario supporting a single-level (OTC provider) and a two-level supply chain consisting of a customer (OTC user) and a supplier (OTC provider). For the single-level scenario, the framework’s results are identical to those of ISO 27001. For the two-level scenario, the framework solves the problem of a lack of effectivity of traditional GRC frameworks regarding federated business scenarios. Given the generic structure of the framework developed, the evaluation could easily be extended to the use of an even deeper layered scenario. Due to the complexity of the OTC, any other End-to-End business processes can be addressed as well. Even without mobile support of the business process in question, general controls can be derived with various protection requirements.

Overall, the framework developed is able to address GRC requirements at the design time of complex End-to-End business processes. Therefore, it addresses the origin of GRC incidents instead of just their symptoms, as traditional information security management systems do. Future research could deliver even more specific control sets for different types of technical resources used to support business processes across organizations.

References


